



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,133	03/13/2000	AHMET MURSIT ESKICIOGLU	RCA88674	9526

24498 7590 08/22/2007
JOSEPH J. LAKS, VICE PRESIDENT
THOMSON LICENSING LLC
PATENT OPERATIONS
PO BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER

PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

08/22/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/445,133

Applicant(s)

ESKICIOGLU, AHMET MURSIT

Examiner

Yogesh Paliwal

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 5/29/2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Docketing

Please note that the application has been redocketed to different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Amendment

- This office action is in response to amendment filed on 5/29/07. The amendment filed on 5/29/07 have been entered and made of record. Therefore, presently pending claims are 1-20.

Response to Arguments

- Applicant's arguments filed on 5/29/07 have been fully considered.
- Regarding independent **claim 1**, applicant argues that: "nowhere do Kaplan and Renaud teach or suggest at least receiving in a device an electronic list of events available from one or more sources each event having a digital signature and an encrypted message associated therewith; receiving in the device, in response to user selection of one of the events, the digital signature and the encrypted message associated with the selected event, the digital signature being encrypted with a first key, the encrypted message being encrypted with a second key different from the first key, and the encrypted message comprising a descrambling key; and authenticating in the device a source of the digital

Art Unit: 2135

signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message, as now recited in independent claim 1”.

- In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (all the underlined limitations) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Applicant should further note that Kaplan and Renaud combination still teach all the limitations including limitations included by last amendment presented in amended claim 1. Refer to the rejection of claim 1 below. As a result, newly presented amendment failed to overcome previously presented Kaplan and Renaud references.
- Regarding independent **claim 15**, applicant argues that: “Many of these features are not taught or suggested by Kaplan, Renaud and Vancelette, whether taken alone or in proper combination. Specifically, none of these documents is understood to teach or suggest passing a message to a smart card, decrypting the message in the smart card using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event information; or descrambling, in

Art Unit: 2135

the smart card, the selected event using the symmetric key to generate a descrambled event."

- Applicant's arguments, with respect to the rejection of independent claim 15 under 103(a) have been fully considered and are persuasive.

Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Macq et al. (Macq, B.M.; Quisquater, J.-J., "Cryptology for digital TV broadcasting," Proceedings of the IEEE , vol.83, no.6, pp.944-957, Jun 1995), hereinafter Macq. Macq with previously presented references now discloses all the limitations that were argued by applicant.

- Regarding independent **claim 18**, applicant argues that: "Independent claim 18 recites a method for managing access between a device having a smart card coupled thereto and a service provider. Among other steps, the method includes passing a message to a smart card; decrypting, in the smart card, the message using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event information and descrambling in the smart card the selected event using the symmetric key to generate a descrambled event. The Office Action fails to consider these features, and none of the documents cited in the rejection of claim 18 even mentions a smart card."

Art Unit: 2135

- Applicant's arguments, with respect to the rejection of independent claim 15 under 103(a) have been fully considered and are persuasive.

Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Macq. Macq with previously presented references now discloses all the limitations that were argued by applicant.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Kaplan ("IBM Cryptolopes, Super Distribution and Digital Rights Management"), hereinafter Kaplan, in view of Renaud (US 6,021,491), hereinafter Renaud.

Regarding **Claim 1**, Kaplan discloses the cryptolope system wherein the user device receives an electronic list of events available from one or more sources (**Page 6, lines 13-16, "A cryptolope is usually acquired or "downloaded" by the user as a result of a "web search", or an Internet "surfing" session, or a cryptolope may be passed to the user by another user or an information gathering service"**), each event having a digital signature and an encrypted message associated therewith (**Figure on page 3, "Authenticity (BOM) with Digital Signatures" can be interpreted**

as “even having a digital signature”, as required by claim limitation and “encrypted part (text)” and “encrypted part (image)” can be interpreted as “encrypted message”, as required by claim limitation.)

receiving in the device, in response to user selection of one of the events from the list of events (Page 6, lines 13-16, “A cryptolope is usually acquired or “downloaded” by the user as a result of a “web search”, or an Internet “surfing” session, or a cryptolope may be passed to the user by another user or an information gathering service”) the digital signature and the encrypted message associated with the selected event (Figure on page 3, each cryptolope contains encrypted message and digital signature), the digital signature being encrypted with a first key (**Page 5, lines 14-17, “The digital signature of the publisher of the cryptolope is computed and appended to the BOM. (the digital signature is computed as the encryption of the cryptographic hash of the BOM under the private key of the publisher using a “public key” algorithm such as RSA.)”**) and the encrypted message being encrypted with a second key different from the first key (**Page 3, lines 7-12, “Each protected part is treated as a file of bytes that is encrypted under a unique, randomly chosen secret *document key* using a relatively efficient “bulk” encryption algorithm such as DES-CBS.”**. Note: It can be seen that digital signature is computed using a private key of the publisher and the message is encrypted with a secret “document key”, as a result, Kaplan teaches a claim limitation that requires second key to be different from the first key),

the encrypted message comprising a descrambling key (**Figure on Page 3, “Key Record”**) and event information (**Figure on Page 3, “Terms and Conditions”**) including at least one a channel identity, date and time stamp, even identity and payment amount corresponding to the selected event (**Page 4, lines 11-24, “Terms and Conditions”**);

authenticating (**Page 5, line 8, “Authentication with Digital Signatures”**), a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message (**Page 5, lines 20-23, “A user or clearing center can verify the authenticity of any part(s) of a cryptolope by first checking the digital signature on the BOM (using information contained in the public key certificate) and then checking that the cryptographic hash values(s) of the part(s) of the cryptolope match the value(s) stored in the BOM.”**);

decrypting in the device, the encrypted message to obtain the descrambling key upon the authenticating (**Page 7, “ “Buying” a Cryptolope”, Parts 7 and 8**);

receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event (**Page 6, Publisher Content Creator Paragraph**); and

descrambling in the device, the selected event using the descrambling key (**Part 8 of “ “Buying” a Cryptolope”, on page 7**).

Although Kaplan discloses the authentication of the digital signature of the provider, the system of Kaplan also discloses the authentication among participants. However Kaplan does not expressly disclose the authentication in the receiving device.

Renaud discloses a method, apparatus, and product for verifying the authenticity of data within one or more data files (**abstract**). Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file (**Column 7 lines 48-62**).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the contents of files as in Renaud using the digital signature and system of Kaplan. One of ordinary skill in the art would have been motivated to do this because digital signature verification provides a relatively high level of confidence in the authenticity of the source of the received data (**Renaud Column 2, lines 1-10**)

Claims 2-14, are rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Kaplan and further in view Renaud as in claim 1 and further in view of Macq.

Regarding Claim 2, the rejection of claim 1 is incorporated and Kaplan further discloses device comprising the steps of decrypting the message, receiving the selected event (**Page 6, lines 13-16, "A cryptolope is usually acquired or "downloaded" by the user as a result of a "web search", or an Internet "surfing" session, or a cryptolope may be passed to the user by another user or an information gathering service"**), and descrambling the selected event (**Page 7, " "Buying" a**

Art Unit: 2135

Cryptolope”, steps 7 and 8). Combination of Kaplan and Renaud does not teach that receiving and descrambling of event are performed in smart card and message is encrypted using the public of smart card and decrypted using the private key of the smart card.

Macq discloses message being encrypted using a public key of the smart card (Page 945, Column 2, lines 10-15, “In other systems [34], where $K_1 \neq K_2$, the encryption transformation, E_{K_1} , may be publicly known because it is a one-way function. In this case, the term K_1 in (1), is seen as a public key (everyone is able to encrypt) but the key K_2 , which is required for an easy decryption is only known by the authorized receivers”. Note: Macq further disclose that authorized receivers include “smart card” to save the private key and perform the security processing on incoming messages, refer to Page 950, lines 40-45, “smart card”) passing the message to the smart card (Page 950, lines 40-41, “These messages are routed to the security processor (implemented for example as a smart card) over the signal transmission channel.”); decrypting, in the smart card, the message using a private key being stored within the smart card (Page 950, lines 42-44, “The security processor will decipher the control word [that is equivalent to the document key of Kaplan]”, Note: it is implied that when public key encryption method is used, as suggested by Macq at page 945, Column 2, lines 10-15, the encrypted data which is encrypted using a public key of the receiver [smart card] can only be decrypted using a private key of the receiver [smart card]).

Art Unit: 2135

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to utilize in the system of Kaplan, smart card attached to the user terminal, as suggested by Macq, because smart cards are small and efficient with increasingly more powerful processing speed. Also smart card provides full protection of the private key, which needs to be in full secrecy all time.

Regarding **Claim 3**, the rejection of claim 2 is incorporated and Kaplan further discloses the message further comprises event information, the event information being decrypted using the private key (**Page 3**).

Regarding **Claim 4**, the rejection of claim 3 is incorporated and combination of Kaplan, Renaud and Macq further discloses step of storing the event information, wherein the step of storing event information is performed in the smart card (**Macq, Page 950, lines 42-44, "The security processor will decipher the control word [that is equivalent to the document key of Kaplan] and supply it to the unscrambling unit if one of the entitlements it contains covers the access parameters appearing in the ECM"**)

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Macq discloses smart card has a card body having plurality of terminals arranged on a surface of the card body in accordance with one of IS) 7816 and PCMCIA card standard (**Note: it is inherent that the card body has terminals on its body for connection to the card reader for accessing the memory of the card**).

Regarding **Claim 6**, the rejection of claim 5 is incorporated and Kaplan further discloses authenticating said list of events to verify the origin of said message. The

Art Unit: 2135

events in the list are authenticated by the virtue of the list are authenticated by the virtue of the list being encrypted by the service provider. The terminal then decrypts the packets with the corresponding key. This implies that only those with the key that corresponds the key of the service provider can decrypt the list and therefore the information comes from the service provider **(page 2)**.

Regarding **Claim 7**, the rejection of claim 6 is incorporated and further Kaplan discloses the use of the private key used for digital signatures for authentication purposes **(page 3)**.

Regarding **Claim 8**, the rejection of claim 4 is incorporated and further Kaplan discloses that event information comprises channel identity data, date and time stamp data and billing data **(page 4)**.

Regarding **Claim 9**, Claim 9 depends from claim 3 and is identical to claim 4 (which also depend from claim 3) and thus rejected on same rational as claim 4 above.

Regarding **Claim 10**, the rejection of claim 7 is incorporated and Kaplan further discloses digital signature, said second public key and said second private key are issued by an independent certificate authority and are associated with said list provider **(page 6)**.

Regarding **Claim 11**, the rejection of claim 10 is incorporated and Kaplan further discloses that discloses the device is a digital television **(The device suggested by Kaplan is a display device, a digital television is a display device (Page 1))**.

Regarding **Claim 12**, the rejection of claim 10 is incorporated and the combination of Kaplan and Macq further discloses that the device is a set-top box **(Macq, Page 945, line 39, "Set-top box")**.

Regarding **Claim 13**, the rejection of claim 4 is incorporated and Kaplan further discloses that the event information is used within the device to update a user's account information **(Page 7, " "Buying" a Cryptolope", step 1)**.

Regarding **Claim 14**, the rejection of claim 13 is incorporated and Kaplan further discloses that the event information is downloaded to an independent billing center to update the user's account information **(Page 7, " "Buying" a Cryptolope", steps 2,3 and 4)**.

Claims 15-17 are rejected under 35 U.S.C 103(a) as being unpatentable over Kaplan in view of Renaud and further in view of Macq.

Regarding **Claim 15**, Kaplan discloses the cryptolope system wherein the user device receive an electronic list of events having a plurality of events, **(Page 6, lines 13-16, "A cryptolope is usually acquired or "downloaded" by the user as a result of a "web search", or an Internet "surfing" session, or a cryptolope may be passed to the user by another user or an information gathering service")**, the list having a message and a digital signature associated with each event in the list **(Page 6, lines 13-16 and Figure of Page 3, it can be seen from the figure that each cryptolope contains message and digital signature)**, the message being encrypted using a key

Art Unit: 2135

(Page 3, line 14, “Each document key is encrypted under a master key”) and the digital signature being created using a private key of the list provider (Page 5, lines 14-17, “The digital signature of the publisher of the cryptolope is computed and appended to the BOM. (the digital signature is computed as the encryption of the cryptographic hash of the BOM under the private key of the publisher using a “public key” algorithm such as RSA.)”);

selecting an event from the list (Page 6, lines 13-16, “A cryptolope is usually acquired or “downloaded” by the user as a result of a “web search”, or an Internet “surfing” session, or a cryptolope may be passed to the user by another user or an information gathering service”);

receiving the encrypted message and the digital signature corresponding to the selected event (Figure of Page 3, with encrypted messages, encrypted keys and digital signature of the provider);

authenticating the list provider by decrypting the digital signature using a public key of the list provider, the list provider public key being stored in the device; (Page 5, lines 20-23, “A user or clearing center can verify the authenticity of any part(s) of a cryptolope by first checking the digital signature on the BOM (using information contained in the public key certificate) and then checking that the cryptographic hash values(s) of the part(s) of the cryptolope match the value(s) stored in the BOM.”);

receiving from the service provider the selected event, the selected event being scrambled using the symmetric key (Page 6, Publisher Content Creator Paragraph);

Although Kaplan discloses the authentication of the digital signature of the provider, the system of Kaplan also discloses the authentication among participants. However Kaplan does not expressly disclose the authentication in the receiving device.

Renaud discloses a method, apparatus, and product for verifying the authenticity of data within one or more data files (**abstract**). Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file (**Column 7 lines 48-62**).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the contents of files as in Renaud using the digital signature and system of Kaplan. One of ordinary skill in the art would have been motivated to do this because digital signature verification provides a relatively high level of confidence in the authenticity of the source of the received data (**Renaud Column 2, lines 1-10**).

Kaplan does not expressly disclose indicating the events that are available to the customer in the form of an electronic list of events.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to indicate to the customer the types of events that are available to the customer in the form of an electronic list of events. One of ordinary skill in the art would have been motivated to do this because a list is an organized and simple way of communicating information.

Kaplan does not disclose:

message being encrypted using a public key of the smart card;

Art Unit: 2135

passing the message to the smart card;

decrypting, in the smart card, the message using a private key of the smart card to obtain event information and symmetric key, the smart card private key being stored within the smart card;

storing the event information in smart card and updating account information based on the event information;

and descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

Macq discloses message being encrypted using a public key of the smart card (Page 945, Column 2, lines 10-15, "In other systems [34], where $K_1 \neq K_2$, the encryption transformation, E_{K_1} , may be publicly known because it is a one-way function. In this case, the term K_1 in (1), is seen as a public key (everyone is able to encrypt) but the key K_2 , which is required for an easy decryption is only known by the authorized receivers". Note: Macq further disclose that authorized receivers include "smart card" to save the private key and perform the security processing on incoming messages, refer to Page 950, lines 40-45, "smart card") passing the message to the smart card (Page 950, lines 40-41, "These messages are routed to the security processor (implemented for example as a smart card) over the signal transmission channel."); decrypting, in the smart card, the message using a private key being stored within the smart card (Page 950, lines 42-44, "The security processor will decipher the control word [that is equivalent to the document key of Kaplan]"; Note: it is implied that when public key encryption method is used,

as suggested by Macq at page 945, Column 2, lines 10-15, the encrypted data which is encrypted using a public key of the receiver [smart card] can only be decrypted using a private key of the receiver [smart card]); storing the event information in smart card and updating account information based on the event information and descrambling in the smart card (Page 950, lines 42-44, "The security processor will decipher the control word [that is equivalent to the document key of Kaplan] and supply it to the unscrambling unit if one of the entitlements it contains covers the access parameters appearing in the ECM");, the selected event using the symmetric key to generate a descrambled event (Page 954, lines 31-32, "If the checking is correct, the ACU gives the descrambler the key to decipher the program").

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to utilize in the system of Kaplan, smart card attached to the user terminal, as suggested by Macq, because smart cards are small and efficient with increasingly more powerful processing speed. Also smart card provides full protection of the private key, which needs to be in full secrecy all time.

Regarding **Claim 16**, rejection of claim 15 is incorporated and the combination of Kaplan, Renaud and Macq further discloses wherein the device is a set-top box (**Macq, Page 945, line 39, "Set-top box"**)

Regarding **Claim 17**, rejection of claim 15 is incorporated and Kaplan further discloses that the device is a digital television (**The device suggested by Kaplan is a display device, a digital television is a display device (Page 1)**).

Claim 18-20 are rejected under 35 U.S.C 103(a) as being unpatentable over the combination of Kaplan in view of Renaud and Schneier and further in view of Macq.

Regarding **Claim 18**, Kaplan discloses the cryptolope system wherein the user device receive an electronic list of events from a provider (**Page 6, lines 13-16, "A cryptolope is usually acquired or "downloaded" by the user as a result of a "web search", or an Internet "surfing" session, or a cryptolope may be passed to the user by another user or an information gathering service")** having a digital certificate (**Page 5, lines 18-19, "Additionally, the public key certificate of the publisher is included as another sub-file of the cryptolope, represented in a standard format such as X.509)** and a separate message corresponding to each event in the list (**Figure at page 3**), each of said digital certificates being encrypted using a first private key of the provider (**Page 5, lines 18-19**), the separate message being encrypted using a key (**Page 3, line 14, "Each document key is encrypted under a master key")** and having a associated digital signature created using a second private key of the provider (**Page 5, lines 14-17, "The digital signature of the publisher of the cryptolope is computed and appended to the BOM. (the digital signature is computed as the encryption of the cryptographic hash of the BOM under the private key of the publisher using a "public key" algorithm such as RSA.)")**

selecting an event from the list (**Page 6, lines 13-16, "A cryptolope is usually acquired or "downloaded" by the user as a result of a "web search", or an Internet "surfing" session, or a cryptolope may be passed to the user by another user or an information gathering service"**);

receiving the digital certificate, the message and the digital signature corresponding to the selected event (**Figure at page 3, and page 5 lines 18-19**)

Kaplan does not expressly disclose indicating the events that are available to the customer in the form of an electronic list of events.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to indicate to the customer the types of events that are available to the customer in the form of an electronic list of events. One of ordinary skill in the art would have been motivated to do this because a list is an organized and simple way of communicating information.

Although Kaplan discloses decrypting a digital signature during the authentication, Kaplan does not disclose using a first public key to obtain a second public key.

Schneier discloses transferring keys using key-encryption keys to encrypt other keys for distribution (**Page 176, section 8.3 paragraph 3**). Therefore decrypting the first key to obtain a second key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a key encryption key to encrypt another key as in Schneier to decrypt the digital signature of Kaplan. One of ordinary skill in the art would have been

Art Unit: 2135

motivated to do this because key encryption key is a common method of distributing keys **(Schneier Page 176, section 8.3, paragraph 3).**

The combination of Kaplan and Schneier does not disclose:
message being encrypted using a public key of the smart card;
passing the message to the smart card;
decrypting, in the smart card, the message using a private key of the smart card
to obtain event information and symmetric key, the smart card private key being stored
within the smart card;
storing the event information in smart card and updating account information
based on the event information;
and descrambling, in the smart card, the selected event using the symmetric key
to generate a descrambled event.

Macq discloses message being encrypted using a public key of the smart card
**(Page 945, Column 2, lines 10-15, "In other systems [34], where $K_1 \neq K_2$, the
encryption transformation, E_{K_1} , may be publicly known because it is a one-way
function. In this case, the term K_1 in (1), is seen as a public key (everyone is able
to encrypt) but the key K_2 , which is required for an easy decryption is only known
by the authorized receivers". Note: Macq further disclose that authorized
receivers include "smart card" to save the private key and perform the security
processing on incoming messages, refer to Page 950, lines 40-45, "smart card")**
passing the message to the smart card **(Page 950, lines 40-41, "These messages are
routed to the security processor (implemented for example as a smart card) over**

the signal transmission channel.”); decrypting, in the smart card, the message using a private key being stored within the smart card **(Page 950, lines 42-44, “The security processor will decipher the control word [that is equivalent to the document key of Kaplan]”**, Note: it is implied that when public key encryption method is used, as suggested by Macq at page 945, Column 2, lines 10-15, the encrypted data which is encrypted using a public key of the receiver [smart card] can only be decrypted using a private key of the receiver [smart card]); storing the event information in smart card and updating account information based on the event information and descrambling in the smart card **(Page 950, lines 42-44, “The security processor will decipher the control word [that is equivalent to the document key of Kaplan] and supply it to the unscrambling unit if one of the entitlements it contains covers the access parameters appearing in the ECM”)**, the selected event using the symmetric key to generate a descrambled event **(Page 954, lines 31-32, “If the checking is correct, the ACU gives the descrambler the key to decipher the program”)**.

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to utilize in the system of Kaplan, smart card attached to the user terminal, as suggested by Macq, because smart cards are small and efficient with increasingly more powerful processing speed. Also smart card provides full protection of the private key, which needs to be in full secrecy all time.

Regarding **Claim 19**, rejection of claim 18 is incorporated and the combination of Kaplan, Renaud and Macq further discloses wherein the device is a set-top box (Macq, Page 945, line 39, "Set-top box")

Regarding **Claim 20**, rejection of claim 18 is incorporated and Kaplan further discloses that the device is a digital television (The device suggested by Kaplan is a display device, a digital television is a display device (Page 1)).

Conclusion

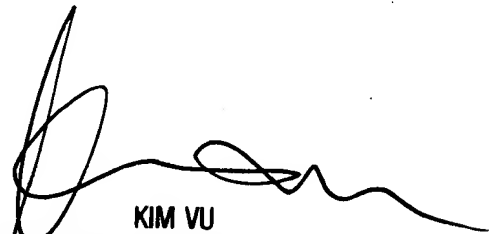
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
8/8/07



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100